



Searchlights

While privacy advocates applaud Google's stand against the US government's demands for search request details, Paul Nesbitt wonders whether it should be keeping all this data in the first place

Google has refused to hand over data it holds on people's search requests to the US government, which wants them as evidence to back its controversial Child Protection Act. To privacy advocates, this is a landmark case that will determine how easily governments can gain access to confidential data companies hold on people and use it for surveillance. It also raises questions about whether or not corporations should even keep such large and varied amounts of customer data.

Google refused to comply with a subpoena issued by the US Department of Justice (DOJ). "Google's acceding to the request would suggest it is willing to reveal information about those who use its services. This is not a perception that Google can accept," wrote Google attorney Ashok Ramani in a letter to the US DOJ on 10th October.

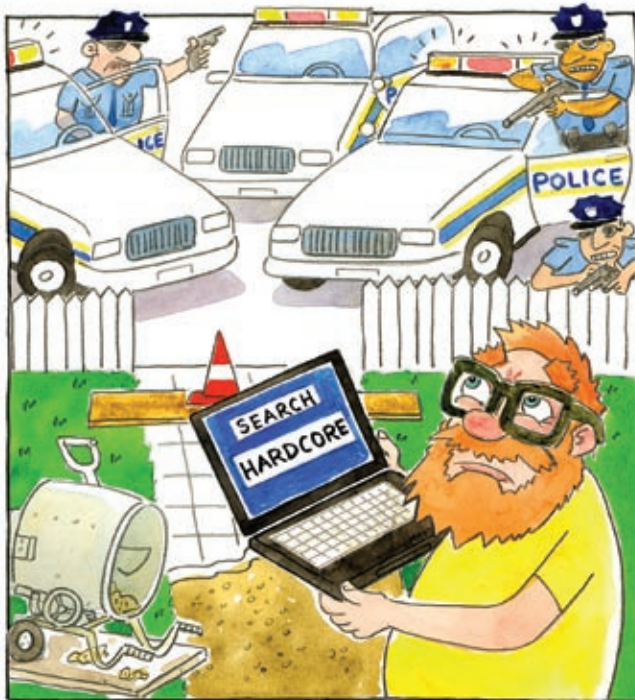
But now the US Attorney General has asked a Federal judge to make Google hand over a list of search requests made during a single week, as well as a million randomly selected web addresses from Google databases. The Bush administration wants the data to help it build a case against the Supreme Court, which struck down the bill in 2004 as unconstitutional and a threat to free speech.

NO HASSLE

Google refused the request, describing it as "overbroad, unduly burdensome, vague and intended to harass". Nicole Wong, an associate general counsel for Google, said that "Google is not a party to this lawsuit, and the demand for the information is overreaching."

US digital privacy campaigner Lauren Weinstein described the outcome of the stand-off as "breathtaking in its potential importance" for the rights of citizens to privacy from governments. Already companies such as Yahoo! and Microsoft have been criticised for aiding the Chinese government's crackdown on dissidents who use the internet. Google itself has agreed to censor content accessible by China. In the US, President Bush has recently come under fire for allegedly using illegal taps on US citizens communicating with foreigners.

"This is exactly the kind of thing we have been worrying about with search engines for some time. Google should be commended for fighting this," said Pam Dixon, the executive director of the World Privacy Forum. "When you are looking at that blank search box, you should remember that what you type into it can come back to haunt you unless you take precautions," she told the Associated Press.



The US government's move is a dry run in preparation for extracting more personal data from search engines in the future

EXTRACTION ENGINE

Many observers have asked why the US government didn't just hire a company to analyse publicly available data on the internet from various archiving services. It seems that the government's move is a dry run in preparation for extracting more personal data from search engines in the future. "We think companies should be pushing back. They're only going to be asked for more," said Ari Schwartz, associate director of the Center for Democracy and Technology. "These things are gradual. They see if they can get what they're asking for, and it gets bigger and bigger," he said.

However, this view of the DOJ request as the thin end of the wedge is not shared by other search giants, including Yahoo!, AOL and Microsoft, none of which sees the US government request as such a big deal. After all, it is only seeking information on the general popularity of keywords and URLs, rather than seeking data on individuals or linking them with their searches. The DOJ claims it wants the data to test the efficacy of filters to stop children visiting porn sites on the internet.

Yahoo! released a statement saying: "We complied with the request on a limited basis and

didn't provide any personally identifiable information. We are rigorous defenders of our users' privacy. We did not provide any personal information in response to the Department of Justice's subpoena."

Microsoft also explained its actions in complying. "We did comply with their request for data in regards to helping protect children in a way that ensured we also protected the privacy of our customers. We were able to share aggregated query data (not search results) that did not include any personally identifiable information."

AOL defended its position in a similar way. "We gave the DOJ a generic list of aggregate and anonymous search terms from a roughly one-day period. This did not include search results nor any personally identifiable information and therefore there were absolutely no privacy implications," it said.

AGENDA BENDER

Ray Everett-Church, a Californian privacy expert, told *The Mercury News* that the case against Google was an "atypical use of subpoena power" because the administration is demanding data to further a political agenda rather than using it to pursue criminals. "It certainly sets a dangerous precedent for the government to say, 'We need this to make a point, so cough up your log data'. It's a remarkable leap for the government, and not one I've seen before."

Everett-Church said there is a trade-off between the benefits sites claim to offer by asking for personal information in order to personalise the online experience, and the danger that such data could be subpoenaed or seized in a warrant by a government.

The fact that Google archives such data will come as an unpleasant surprise to many people. "It's interesting and disappointing that other search engines would provide this material," said Weinstein. "It's what we've been worried about all along. My initial reaction is three cheers for Google. But there is a sidebar to this. Part of the reason these problems come up is because this data is being retained in the first place."

Weinstein also warned Europeans not to feel complacent. A December vote by the European Parliament forces ISPs and telecoms companies to hold data on IP locations and phone numbers called for up to two years. National police and intelligence agencies will have the automatic right to access the data. However, the legislation is not due to be implemented for 18 months in the case of phone calls, and three years for internet information. **CS**